St Thomas More RC College

Policy:

E-Safety Policy / Acceptable Use Policy (AUP)

This policy will be reviewed every 12 months

Author	J Kirk-HB

	Signature of member of Governing body	Date
Policy approved/ reviewed (delete as appropriate)		October 2026

Rationale

Technology, including the internet, digital platforms and Artificial Intelligence (AI) tools, has become integral to the lives of children and young people, both within school and in their lives outside school. These technologies are powerful resources that offer significant educational and social opportunities; however, their use can also expose young people to risk if not managed appropriately. Pupils are entitled to safe, secure and responsible access to digital technologies at all times.

Potential risks associated with online and digital technologies, including AI, include:

• Access to illegal, harmful or inappropriate images, content or AI-generated material.
• Unauthorised access to, loss of, or sharing of personal or sensitive information.
• The risk of grooming or inappropriate influence through online platforms or AI-enabled communication tools.
• The creation, sharing or distribution of personal images, videos or AI-generated content without an individual's consent or knowledge.
• Inappropriate communication or contact with others, including strangers, through digital or AI-supported services.
• Cyber-bullying, harassment or intimidation, including the use of AI to generate or manipulate content.
• Access to unsuitable websites, videos, online games or AI tools that are not age-appropriate.
• An inability to evaluate the quality, accuracy, bias or reliability of online or AI-generated information.
• Plagiarism, academic dishonesty and copyright infringement, including misuse of AI to generate work presented as a pupil's own.
• Illegal downloading or sharing of digital content.
• Excessive screen time or over-reliance on online or AI tools, which may negatively impact social, emotional development and learning.
• Youth-produced imagery, including digitally altered or AI-generated images.
• Up-skirting and the misuse of digital technologies to invade privacy.

Ensuring that children and young people are able to use the internet, digital technologies and AI tools appropriately and safely forms part of the school's wider duty of care and safeguarding responsibilities. All staff have a responsibility to promote safe practice, model appropriate behaviour and respond promptly to concerns related to online or AI-related risks.

This policy aims to support safe and appropriate use of digital technologies, including AI, and to encourage pupils to become discerning, responsible and informed users. It should be read in conjunction with the Child Protection Policy, the Anti-Bullying Policy and the Behaviour Policy.

This e-safety policy has been developed by the E-safety Team made up of:

Position	Name(s)
Head of Learning Support	Joanne Kirk Child Protection Teacher
Curriculum Leader – Computer Science	Adam Jennings
Curriculum Leader – CPSHE	Liam Wright
HLTA Inclusion	Kiayah Nolan
IT Support	Dataspire (Lee Owen -Taylor)

Consultation with the whole college community has taken place through the following:

Staff meetings
INSET Day – Annual Staff Training – Staff sign Safeguarding Agreement

This policy applies to all members of the college community (including governors, staff, students/pupils, volunteers, parents/carers, visitors, community users) who have access to and are users of the college ICT systems and mobile technologies, both in and out of college.

Roles and Responsibilities

The following section outlines the roles and responsibilities for e-safety of individuals and groups within the college:

Governors:

- Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy.

Head Teacher and Senior Leaders:

- The Head Teacher/Deputy Head Teacher are responsible for ensuring the safety (including e-safety) of members of the college community.
- The Head Teacher and the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

E-Safety Team:

- Members of the E-safety Team will assist the E-Safety Coordinator with the production, review and monitoring of the college e-safety policy on an annual basis.

DSL/DDSL:

- leads the e-safety Team and college initiative on e-safety.
- takes day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the college e-safety policies.
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- provides training and advice for staff.

- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments.
- reports regularly to the Senior Leadership Team**.**

Joanne Kirk is trained in e-safety issues and is aware of the potential for serious Child Protection issues to arise from:

- sharing of personal data.
- access to illegal/inappropriate/ extremist materials.
- inappropriate on-line contact with adults/strangers.
- potential or actual incidents of grooming e.g. Child Sexual Exploitation, radicalisation.
- cyber-bullying.

Network Manager / Technical staff:

Dataspire is responsible for ensuring:

- that the college's ICT infrastructure is secure and is not open to misuse or malicious attack.
- that the college meets the e-safety technical requirements outlined in any relevant Government/DfE and Local Authority guidance.
- that users may only access the college's networks through a properly enforced password protection and AUP policy.
- that security, safeguarding and network filtering systems are suitable and up to date.
- that the college cloud/ internet-based services are suitably secure.
- that appropriate backup solutions are in place and regularly tested.
- ensuring the college complies with data protection and GDPR regulations.

Teaching and Support Staff:

are responsible for ensuring that:

- they have an up-to-date awareness of data protection and e-safety matters and of the current college e-safety policy and practices.
- they have read, understood and electronically signed the college Staff Acceptable Use Policy/Agreement (AUP), at the beginning of each half term.
- they report any suspected misuse or problem to the E-Safety Co-ordinator (J Kirk) for investigation/action/sanction.
- they have read all relevant safeguarding documents and signed to confirm this annually.

Pupils:

- are responsible for using the college ICT systems and other school provided technologies in accordance with the Pupil Acceptable Use Policy, which they sign electronically when logging in to college systems.
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so and who to report to.

Parents/Carers

The college will take every opportunity to help parents understand these issues through website information about national/local e-safety campaigns. Parents and carers will be responsible for:

- endorsing (by signature) the STM Student IT Services Agreement as part of the admission process.
- accessing the college ICT systems in accordance with the procedures set out within this policy.

Communication devices and methods

The following table shows the college's policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table. For the avoidance of doubt though, from time to time, any measures in the school behaviour policy that relate to mobile technology or other electronic devices supersedes any information within this policy, as the behaviour policy may be updated more regularly.

	Staff & other adults				Pupils			
Communication method or device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
	☑	⚠	⚠	☒	☑	⚠	⚠	☒
Only school Approved "Brick" Mobile phones may be brought to college by students but must be switched off in bag and only used on journey to and from school. Smart Devices are not permitted to be brought onto the school site by students							⚠	
Use of mobile phones in lessons. For staff Only for legitimate educational purposes such as MFA		⚠						☒
Staff use of mobile phones in social time away from student areas		⚠						☒
Taking photos or videos on personal mobile phones or other camera devices				☒				☒
Interactive use of wearable electronic devices e.g. Smart watches, o		⚠						☒
Use of tablet devices for educational purposes	☑						⚠	
Use of personal email addresses in college, or on college network		⚠						☒
Use of college email for personal emails				☒				☒
Use of online meetings (Teams, Zoom, Satchel One) chat rooms / messaging facilities for educational purposes	☑						⚠	
Use of social networking sites				☒				☒
Use of educational blogs/vblogs (YouTube etc)	☑						⚠	

 This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
Communication method or device	**Staff & other adults**	**Pupils**
Only school Approved "brick" Mobile phones may be brought to college but must be switched off in bag and only used on journey to and from school		School approved phones must not be used at all on school premises and can only be used on the journey to and from school in line with the school's behavior policy. In emergency circumstances a student may be given permission to use an approved mobile phone by a member of staff. Smart Devices should not be brought onto school site by pupils in line with the school behaviour policy
Use of mobile phones in social time	During breaks/lunch or after college. Phones must not be used in the presence of students unless an emergency or for an educational purpose.	
Use of personal tablets and handheld devices	As a teaching resource	As a focused learning resource, monitored by teachers
Use of personal email addresses in college, or on college network	During breaks/lunch or after college	
Use of college email for personal emails	College emails are not to be used for personal business and communication.	As a learning resource to send work home and collaborate with other students *remove as this could be a security risk for malware
Use of online meetings (Teams, Zoom, Satchel One) chat rooms / messaging facilities for educational purposes	Contact staff within school, or to communicate with external agencies e.g. webinars (training)	As a learning resource in lessons
Use of educational blogs/ video sites/podcasts (YouTube etc)	Access teaching resources	Use as a learning tool.

Unsuitable/inappropriate activities using college internet & devices

The college believes that the activities referred to in the following section would be inappropriate in a college context and that users, as defined below, should not engage in these activities in college or outside college when using college equipment or systems. Internet access on site is monitored and filtered, in order to restrict access to inappropriate material. The college policy restricts certain internet usage as follows:

	Acceptable	Acceptable at certain times	Acceptable for nominated users (staff)	Unacceptable	Unacceptable and illegal
User Actions	☑			☒	☒
child sexual abuse images					☒
promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					☒
adult material that potentially breaches the Obscene Publications Act in the UK					☒
criminally racist material in UK					☒
Extremist materials					☒
Pornography					☒
promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					☒
promotion of racial or religious hatred					☒
threatening behaviour, including promotion of physical violence or mental harm					☒
any other information which may be offensive to colleagues or breaches the integrity of the ethos of the college or brings the college into disrepute				☒	
Using college systems to run a private business				☒	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by STM and / or the college				☒	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				☒	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					☒
Creating or propagating computer viruses or other harmful files					☒

Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet				☒	
On-line gaming (educational)					
On-line gaming (non-educational)				☒	
On-line gambling				☒	
Accessing the internet for personal or social use (e.g.online shopping, banking etc.)					
File sharing e.g. Music, films etc.				☒	
Use of social networking sites				☒	
Use of video broadcasting e.g.YouTube					
Using external data storage devices (e.g.USB) that have not been encrypted (password protected and checked for viruses)				☒	
The storage of sensitive/inappropriate documents/media files of any description on the college cloud-based storage solutions					☒

 This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
User Actions	**Staff & other adults**	**Students/Pupils**
On-line gaming (educational)		as a learning resource
Accessing the internet for personal or social use (e.g. online shopping, banking etc.)	during break/ lunch times and in personal time	
File sharing e.g. music, films etc.		only if copyright-free to complete the necessary learning activity
Use of video broadcasting e.g. YouTube	for showing educational videos	as a learning resource, to access tutorials
Using external data storage devices (e.g. USB/Cloud based storage) that have not been encrypted (password protected and checked for viruses)	used to save teaching and learning materials only for use at home	used to save work for home learning

Use of Artificial Intelligence (AI) – E-Safety

The school recognises that AI tools are widely accessible and can present online safety risks. All pupils and staff must use AI safely, responsibly, and ethically.

Pupils must:

- Use AI only for school-approved, educational purposes
- Keep personal information, images, and videos private
- Think critically about AI outputs and report anything unsafe or inappropriate
- Never use AI to impersonate others or create harmful content

Staff must:

- Ensure AI use is age-appropriate and supervised
- Check AI content before sharing with pupils
- Protect pupil data and follow professional conduct standards
- Teach pupils about AI risks, including misinformation and bias

Staff must not:

- Enter pupil personal private data, safeguarding information, private assessment data, or confidential school information into public AI platforms unless the service or action has been approved by SLT

General rules:

- AI must not replace trusted adult support or professional judgement
- Any concerns or misuse must be reported to the DSL
- Only school-approved AI platforms may be used for processing data such as Microsoft Copilot as part of RM unify or ChatGPT, if you wish to use another AI platform for processing data please request permission from SLT

This guidance supports existing e-safety, safeguarding, and data protection policies and will be reviewed regularly.

Good practice guidelines

Email

Best practice

☑ DO

Staff and students/pupils should **only** use their college email account to communicate with each other, when necessary. Information shared should relate to school matters unless permission is sought from the Headteacher to share other matters.

Safe practice



Check the college e-safety policy regarding use of your college email or the internet for personal use e.g. shopping/ social media

Poor practice

☒ DO NOT

- **Staff:** don't use your personal email account to communicate with students/pupils and their families without SLT knowledge or permission – and in accordance with the e-safety policy. If email has to be used ensure that this is your school email

Images, photos and videos (media files)

Best practice

☑ DO

- Only use college equipment for taking pictures and videos.
- Ensure parental permission is in place.

Safe practice



- Check the e-safety policy for any instances where using personal devices may be allowed.
- Always make sure you have the Head Teacher/SLT knowledge or permission
- Make arrangements for pictures to be downloaded to the college network immediately after the event.
- Delete images from the camera/device after downloading.

Poor practice

☒ DO NOT

- Don't download images from organisation equipment to your own equipment.
- Don't use your own equipment without Head Teacher/SLT knowledge or permission – and in accordance with the e-safety policy.
- Don't retain, copy or distribute images for your personal use.

Cameras/ Smart Phone/Smart Devices/ Webcams

Best practice

☑ DO

- Make sure you know about inbuilt software/ facilities and switch off when not in use.
- Store images in a secure location
- Encrypt electronic images before they are stored
- Only use devices belonging to STM college to take and store photos and recordings of children
- Make sure anyone who takes or uses images of children has permission to do so.
- Only keep images/ videos for as long as they have an intended purpose

Safe practice



- Check the e-safety policy for any instances where using personal devices may be allowed.
- Always make sure you have the Head teacher/SLT knowledge or permission
- Plan for pictures saved to be downloaded to the college network immediately after the event.
- Delete images from the camera/device after downloading.

Poor practice

☒ DO NOT

- Don't download images from organisation equipment to your own equipment.
- Don't use your own equipment without Head Teacher/SLT knowledge or permission – and in accordance with the e-safety policy.
- Don't retain, copy or distribute images for your personal use.

Use of **school computer rooms** and **appropriate internet use**

It is mandatory for staff to use **IMPERO** to monitor student activity. Computer rooms should only be used when the learning activity is linked to a specific planned curriculum topic requiring computer access.

If using the internet in **computer led activities pupils must**:

1. be directed to websites or web-searches that are relevant to the topic being studied.
2. **MUST NOT** be allowed to **complete free-style unfocused research** as this potentially creates issues with students deliberately or accidentally searching for content that is then flagged by Impero requiring follow up from the pastoral team.
3. Supervision using the Impero Console and classroom observation must take place when using a computer room or a child is using a laptop in a lesson.
4.

Best practice

☑ DO

- Understand how to search safely online and how to report inappropriate content.
- Make sure you know how to use the Impero Console to monitor lessons being taught in computer rooms.
- Plan for learning by providing pupils with **directed websites** that are **age-appropriate** for the topic being taught

Safe practice



- Staff and students/pupils should be aware that monitoring software will log online activity.
- Be aware that keystroke monitoring software does just that. Any inappropriate usage will be recorded and appropriate sanctions put in place.

Poor practice

☒ DO NOT

- **Allow pupils to freestyle internet searches** as part of the lesson.
- Accessing or downloading inappropriate or illegal material may result in criminal proceedings
- Breach of the e-safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions.

Use of Mobile phones

Best practice

☑ DO

Staff:

- *If you need to use a mobile phone while on college business (trips etc.), the college will should provide equipment for you.*
- *Make sure you are aware of app content and facilities.*

Staff: *Good practice is to have phone on silent while on the school premises, phones should only be used for educational purposes such as MFA*
Pupils: *Smart Phones, Cameras, Smart Watches and Headphones are not permitted on the school site. Only school approved phones may be brought onto the school site and should be switched off at all times and kept securely in bags. Approved phones can only be used on the journey to and from school. Phones will be confiscated in line with the school behaviour policy.*

Safe practice



Check the e-safety policy for any instances where using personal phones may be allowed.

Staff: Disable caller-ID if using to phone to contact external agencies or parents/ carers

Poor practice

☒ DO NOT

Staff:

- Don't use your own phone without the Head Teacher/SLT knowledge or permission. Unless for agreed purpose
- Do not use your mobile phone while pupils are present, unless for educational agreed purpose, e.g. MFA.
- Don't retain student/pupil/parental contact details for your personal use.

Social Media Sites (various)

Best practice

☑ DO

Check all settings and make sure your privacy settings are set to 'Private'.

Ask family and friends to not post tagged images of you on 'Public' profiles.

Safe practice



Don't accept people you don't know as friends.

Be aware that belonging to a 'group' can allow access to your profile.

Poor practice

☒ DO NOT

Don't have an 'Public' profile that includes inappropriate personal information and images, photos or videos.
Staff:

- Don't accept students/pupils or their parents as friends on your personal profile.

Staff:
Don't accept ex-students/ pupils/ parents as friends.

Don't write inappropriate or indiscrete posts about the college, colleagues, students/pupils or their parents.

Incident Management

Incidents (PUPILS):	Refer to e-safety Team	Refer to class teacher	Refer to Head of Department / PAL	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security	Inform parents / carers	Removal of network / internet access rights	Warning	sanction eg detention /confiscation/ exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Unauthorised use of non-educational sites during lessons		☑							☑	☑
Unauthorised use of mobile phone/digital camera / other handheld device Smartphones and smartwatches are not permitted on the school site for students in line with school behaviour policy.		☑	☑	☑			☑			☑
Unauthorised use of social media/ instant messaging/personal email		☑	☑							☑
Unauthorised downloading or uploading of files		☑				☑		☑		☑
Allowing others to access college network by sharing username and passwords			☑				☑	☑		☑
Attempting to access or accessing the college network, using another student's/pupil's account	☑					☑	☑	☑		☑
Attempting to access or accessing the college network, using the someone else's account other than your own.	☑		☑			☑	☑	☑		☑
Corrupting or destroying the data of other users						☑				☑
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☑		☑				☑			☑
Continued infringements of the above, following previous warnings or sanctions	☑			☑						
Actions which could bring the college into disrepute or breach the integrity of the ethos of the college				☑			☑			
Using proxy sites/VPNs or other means to subvert the college's filtering system	☑			☑		☑	☑			☑
Accidentally accessing offensive/ extremist or pornographic material and failing to report the incident	☑		☑			☑	☑			
Deliberately accessing or trying to access offensive/ extremist or pornographic material	☑		☑	☑		☑	☑	☑		
Receipt or transmission that infringes copyright or Data Protection Act		☑								

Incidents (STAFF):	Refer to e-safety Team	Refer to Head of Department / Head of Year / other	Refer to Head teacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Warning	Further sanction *(AT Head Teachers discretion)*
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	☑	☑	☑		☑		
Excessive or inappropriate personal use of the internet / social media sites / messaging / personal email accounts		☑	☑				
Unauthorised downloading or uploading of files	☑		☑		☑		
Allowing others to access college network by sharing username and passwords or attempting to access or accessing the college network, using another person's account	☑	☑	☑		☑		
Careless use of personal data eg holding or transferring data in an insecure manner					☑		
Deliberate actions to breach data protection or network security rules		☑	☑		☑		
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		☑	☑		☑		
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	☑	☑	☑		☑		
Making offensive or defamatory comments through social media or digital communications.			☑				
Using **personal** email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	☑	☑	☑		☑		
Actions which could compromise the staff member's professional standing			☑				
Actions which could bring the college into disrepute or breach the integrity of the ethos of the college			☑				
Using proxy/VPN sites or other means to subvert the college's filtering system		☑	☑		☑		
Accidentally accessing offensive or pornographic material and failing to report the incident							
Deliberately accessing or trying to access offensive or pornographic material	☑		☑	☑			
Breaching copyright or licensing regulations		☑					
Using college systems to run a private business			☑		☑		
Continued infringements of the above, following previous warnings or sanctions			☑				

Further Information - IMPORTANT

Staff - Using social media Responsibly

Your personal activities must not undermine the college's reputation, your professional reputation, or create perceptions of impropriety in the college, or bring the college in to disrepute.

TOP TIPS TO KEEP YOU SAFE (PLEASE READ CAREFULLY)

1) Do not "speak" for the college unless you have express permission…

- You should not "speak" for the college (disclose information, publish information, make commitments/comments or engage in activities on behalf of the college) unless you are specifically authorised to do so by the SLT.

- Any online activities associated with work for the college should be discussed and approved in advance by the SLT.

2) Keep confidential…

- Avoid sharing any confidential information about or dealings with the college, Governors, other employees, and/or members of the public unless you have express written permission from the SLT.

3) If you can be linked to the college act appropriately...

- Where you are clearly identifiable as being an employee of the college and/or discuss your work or college business using social media, you must behave appropriately and in ways that are consistent with the colleges values and policies, avoiding any activities which might bring the college into disrepute.

- Never make offensive or defamatory comments about any parents, children, members of staff or governors. Don't use ethnic slurs, personal insults, obscenity or behave in ways that would not be acceptable in the workplace which could bring the college into disrepute, break the law and leave you open to prosecution and/or disciplinary action.

4) Consider contact with pupils and parents carefully

- Ensure than any contact with pupils (current or former) is strictly within an educational context, if necessary, at all.

- **You are strongly advised not to accept pupils as "friends" on social media sites** for your own protection, if you do liaise with pupils electronically, you are advised to do so using official college email accounts, or managed learning platforms, so that any communication is logged and can be monitored, and remains within the acceptable boundaries of that professional relationship.

- If you receive contact from a pupil (current or former), you are advised to inform your head teacher who will decide about informing their parent(s)/ carer(s), as there are specific rules which apply to use and misuse of social media sites for young people.

- If, despite your best efforts, your personal details fall into the wrong hands and a pupil (current or former) makes contact with you, you should let the SLT know and do not reciprocate this communication.

- Remember the boundaries of your professional relationship with pupils and ensure that your behaviour does not blur these boundaries.

5) Remember that colleagues, prospective employers, parents and children may see your online information…

- Whether you identify yourself as an employee of the college or not, think carefully about how much personal information you want to make public and make sure your profile and the information you post reflects how you want them to see you both personally and professionally.

- It is recommended that you apply the highest privacy settings and regularly review them, as the website may alter the setting without your knowledge.

- Ensure that anything you post is in accordance with the college's E-Safety Policy / Acceptable Use Policy (AUP) and your code of conduct.

- Be aware that inappropriate or derogatory comments about colleagues, Governors, parents or children could potentially lead to gross misconduct, which could ultimately result in dismissal.

6) Choose your "friends" carefully

- You may appear in photographs published by other people, and you may be identified without consent, for example by 'tagging' on Facebook, so you are advised to be mindful of what photographs you appear in.

- You can remove your identification from such photographs but not the photograph itself. Your 'friend' may not have as rigorous security settings as you might choose for yourself.

- If you find out that through no fault of your own, you have been identified in a way which might be in breach of these guidelines, you must take immediate steps to rectify the situation. For example, by contacting the person who published the information / image and asking them to remove it.

7) Stay legal

- Be aware that confidentiality, libel, defamation, copyright and data protection laws apply on-line just as in any other media.

- Remember you are personally liable for what you publish online.

8) Protect yourself from identity fraud...

- Restrict the amount of personal information that you give out.

Acceptable Use of Artificial Intelligence (AI)

Artificial Intelligence (AI), including generative AI services such as **ChatGPT and Microsoft Copilot**, can be valuable educational and productivity tools when used appropriately.

The school recognises that pupils will encounter AI throughout further education, employment and everyday life. Our approach is therefore to teach pupils how to use AI **safely, responsibly, critically and honestly**, rather than simply preventing its use.

AI should be used to **support learning and professional judgement, not replace them**.

Only AI services approved by the school may be accessed using school systems, devices or accounts.

ACCEPTABLE USE OF AI

Pupils may use AI to:

- Ask for explanations of topics or concepts they do not understand.
- Ask for a subject to be explained in a different or simpler way.
- Generate revision questions, quizzes and flashcards.
- Practise questions and receive example answers for comparison.
- Generate ideas or starting points for creative work.
- Brainstorm topics, titles, themes or approaches to a task.
- Help structure an essay, report, presentation or project.
- Create an outline which the pupil then develops themselves.
- Improve spelling, punctuation and grammar where permitted by the teacher.
- Ask for feedback on work they have already written.
- Ask how a piece of work could be improved rather than asking AI to replace it.
- Practise languages and conversations.
- Receive assistance with coding, including explanations of programming concepts and debugging.
- Explore different viewpoints or arguments around a subject.
- Summarise non-assessed information as an aid to revision.
- Generate practice examples in subjects such as mathematics, computing and science.
- Use AI for accessibility and learning support where approved by appropriate staff.
- Learn about AI itself, including its capabilities, limitations, bias and potential risks.
- Use AI as part of a lesson or activity when instructed by a member of staff.

Pupils must remain responsible for the work they produce and should be able to explain and demonstrate their understanding of anything submitted in their name.

Information produced by AI must not automatically be assumed to be correct. Important facts, quotations, references, calculations and sources should be independently checked.

Staff may use AI to:

- Assist with lesson planning or assessment including AI self-marking assessments
- Generate ideas for lesson activities.
- Develop worksheets, quizzes and revision resources.
- Produce differentiated versions of educational material.
- Generate example questions or model exercises.
- Create initial drafts of teaching resources.
- Summarise non-confidential information.
- Assist with administrative tasks.
- Draft generic letters, notices or communications.
- Improve the clarity, spelling, grammar or tone of written material.
- Brainstorm ideas for assemblies, projects or extracurricular activities.
- Assist with curriculum planning.
- Generate examples or explanations for classroom use.
- Develop training materials.
- Help create scripts, presentations and educational content.
- Assist with coding, scripting, formulas and other technical work.
- Research a subject or identify areas for further investigation.
- Generate ideas for supporting different learning needs, provided no identifiable pupil information is supplied.
- Reduce repetitive administrative workload where appropriate.

AI-generated material used by staff must be reviewed by the member of staff before it is distributed or relied upon.

The member of staff remains responsible for the accuracy, suitability and professionalism of any material produced with the assistance of AI.

PROHIBITED USE OF AI

The following uses of AI are **not permitted under any circumstances unless specifically authorised through an appropriate formal school process.**

Personal, confidential or sensitive information

Users MUST NOT enter, upload or disclose personal, confidential or sensitive information into public or unapproved AI services.

This includes, but is not limited to:

- Pupil names where they can identify an individual.

- Dates of birth.
- Home addresses.
- Telephone numbers.
- Personal email addresses.
- Photographs or video of identifiable pupils.
- Medical information.
- Special Educational Needs or Disability information.
- Education, Health and Care Plan information.
- Safeguarding records or concerns.
- Child protection information.
- Specific details of behavioural records.
- Attendance records relating to identifiable pupils.
- Examination candidate information.
- Social care information.
- Family circumstances.
- Counselling or pastoral records.
- Staff personnel information.
- HR records.
- Payroll information.
- Passwords.
- Authentication codes.
- API keys.
- Security credentials.
- Confidential school documents.
- Information relating to active investigations.

Information should be anonymised before AI is used wherever possible.

Safeguarding and pastoral decisions

AI MUST NOT be used to:

- Decide whether a safeguarding referral should be made.
- Determine whether a pupil is at risk.
- Assess the credibility of a pupil making a disclosure.
- Decide the appropriate response to a safeguarding disclosure.

- Replace communication with the Designated Safeguarding Lead.
- Diagnose a pupil with a medical, psychological, behavioural or developmental condition.
- Determine whether a pupil has Special Educational Needs.
- Make decisions about a pupil's welfare or safety.

AI may assist a trained professional in finding general information, but **the decision and responsibility must remain with appropriately qualified school staff**.

Behaviour, discipline and other significant decisions

AI MUST NOT independently make decisions concerning:

- Pupil sanctions or exclusions.
- Behaviour outcomes.
- Admissions.
- Staff recruitment.
- Staff disciplinary action.
- Performance management.
- Safeguarding decisions.
- SEND provision.
- Examination access arrangements.
- Academic grading.
- Any other decision that could have a significant effect on an individual.

AI may provide administrative assistance, but it must not replace human professional judgement.

School work and academic honesty

Pupils MUST NOT:

- Submit AI-generated work and claim it as their own.
- Ask AI to complete homework which they are expected to complete themselves.
- Ask AI to write an entire essay, coursework submission or assignment and submit it as their own work.
- Use AI to disguise plagiarism.
- use AI to rewrite copied material in an attempt to avoid plagiarism detection.
- Fabricate references, quotations, research or sources using AI.
- Use AI where a teacher has specifically prohibited its use.
- Use AI during examinations or controlled assessments where it is not permitted.

- Use AI to circumvent examination or awarding-body regulations.

Where AI use is permitted within assessed work, pupils must follow the requirements of the relevant awarding body and instructions given by their teacher.

Where required, pupils must acknowledge their use of AI and retain evidence of the prompts and responses used.

AI-assisted work must still be the pupil's own work.

Examinations and formal assessments

AI MUST NOT be accessible during an examination unless its use has been explicitly authorised under the rules of the relevant awarding body.

AI must not be used to produce work which is subsequently presented as being solely the candidate's own work.

For GCSE, GCE, vocational or other regulated qualifications, the school's examination and malpractice procedures and the rules of the relevant awarding organisation take precedence over this policy.

Impersonation, deepfakes and deceptive content

AI MUST NOT be used to:

- Impersonate another pupil.
- Impersonate a member of staff.
- Impersonate the school.
- Create fake communications purporting to come from the school.
- Clone or imitate another person's voice without permission.
- Create fake images or video of another person.
- Create sexually explicit or intimate images of any person.
- Alter photographs or video for the purpose of bullying, harassment or humiliation.
- Manufacture evidence against another person.
- Deliberately spread false or misleading information.

Creating, requesting or distributing such content may also constitute a safeguarding, disciplinary or criminal matter.

Bullying, harassment and harmful content

AI MUST NOT be used to:

- Bully, intimidate, threaten or harass another person.
- Generate abusive or discriminatory material.
- Generate sexual content.

- Generate content promoting self-harm.
- Generate extremist material.
- Create deliberately distressing content targeted at another person.
- Produce malicious rumours about pupils or staff.
- Circumvent the school's filtering or monitoring systems.

Normal school behaviour, safeguarding and acceptable-use policies apply equally to AI-generated content.

Cyber security and misuse

AI MUST NOT be used to:

- Attack or attempt to compromise school systems.
- Discover or exploit security vulnerabilities without explicit authorisation.
- Obtain passwords or credentials.
- Generate phishing attacks against pupils, staff or third parties.
- Create malware, ransomware or other malicious software.
- Circumvent network security.
- Circumvent web filtering or monitoring.
- Gain unauthorised access to systems or accounts.
- Conceal activity from the school's monitoring systems.
- Provide confidential details of the school's security infrastructure to external AI systems.

Legitimate cyber-security education must only take place within environments and activities authorised by teaching or IT staff.

AI must not be treated as an authoritative source

Users must not assume that information produced by AI is correct simply because it appears convincing.

AI can produce:

- Incorrect information.
- Invented facts.
- Fake quotations.
- Non-existent books, websites or academic papers.
- Incorrect calculations.
- Out-of-date information.
- Biased information.
- Inappropriate material.

Users should verify important information using appropriate reliable sources.

Approved AI services

Access to AI through school systems is restricted to services approved by the school.

At present, approved services include:

- **ChatGPT**
- **Microsoft Copilot**

Additional AI services may be approved following appropriate consideration of safeguarding, privacy, data protection, security and educational suitability and providing permission is granted from SLT for its use.

The existence of an AI service on the internet does not mean that it is automatically approved for use within school.

Users must comply with any age restrictions and terms of use applying to an approved service.

The key principle

The school expects users to follow a simple principle when using AI:

Use AI to help you think — not to avoid thinking.

AI can explain, suggest, question, assist, check and inspire.

It must not be used to cheat, deceive, harm others, compromise personal information or replace the professional judgement of school staff.

Where a pupil or member of staff is unsure whether a particular use of AI is acceptable, they should seek advice from an appropriate member of staff before using it.